Alle praktijkgerichte artikels hebben we gebundeld in de rubriek 'Doe het zelf'. Vragen? Opmerkingen? Tips? Stuur ze naar Clickx Brieven, Minoc Business Press, Everdongenlaan 15 bus 1, 2300 Turnhout. Je kan ook faxen naar 014/44.20.66 of mailen naar brieven.clickx@minoc.com.

## IN DIT NUMMER



## MOEILIJK? MAKKELIJK?

In de 'Doe het zelf'-rubriek vind je zowel bijdragen voor beginners als voor mensen die al aardig overweg kunnen met hun computer. We hebben een systeem bedacht waarmee je in één oogopslag kan zien hoe moeilijk of makkelijk een artikel is. Zo weet je meteen of het een makkie wordt of dat je er toch even al je concentratie voor nodig hebt...

★☆☆ VOOR BEGINNERS
★★☆ VOOR IEDEREEN
★★★ VOOR GEVORDERDEN

# Brief van de week

De Clickx-redactie wordt elke dag overstelpt met vragen van lezers. Sommige problemen zijn te specifiek om in het magazine te behandelen, maar andere vragen zijn dan weer zo interessant dat ze meer verdienen dan een kort antwoordje. Daarom selecteren we vanaf nu voor elke Clickx Magazine een vraag van een lezer, die we dan uitwerken in een complete workshop. De vraag vind je op deze pagina, de workshop staat op de volgende twee pagina's. Veel plezier!

## Veilig testcircuit




**Overal vind je tips om gratis programma's te downloaden en uit te proberen. Maar tegelijk bots je continu op waarschuwingen om niet zomaar alles te installeren, wegens te riskant! Hoe kan je nu toch allerlei programma's zonder (veel) risico – en moeite – uittesten?**

HUGO VAN DEN BOSSCHE

Op de redactie, waar we dagelijks nieuwe software uitproberen, begrijpen we perfect wat je bedoelt. Ons geheim? Een image van een maagdelijke Windows-installatie, die we in pakweg 5 minuten via het netwerk weer op onze pc hebben losgelaten: gedaan met problemen! Voor de doorsnee thuisgebruiker misschien minder evident, maar er bestaan gelukkig nog andere oplossingen voor wie veel én veilig nieuwe software wil verkennen...





# Veilig testcircuit - Workshop



Stel even dat je met een druk op de knop letterlijk álle schrijfoperaties naar een veilige plek kan omleiden. Dat zou het gedroomde testcircuit zijn voor het proefdraaien van nieuwe tools, of zelfs voor je surftochten naar minder koosjere plekjes ;-). Binnen zo'n beveiligde sessie wordt er namelijk geen bít naar je schijf geschreven – en dus ook niet naar het register of naar je browsergeschiedenis. Nog een druk op de knop, en je belandt weer in de normale Windows-modus, zonder het minste spoor van je experimenten. Dit scenario is ongeveer wat je van ShadowSurfer, en van grotere broer ShadowUser Pro, mag verwachten. Beide tools komen trouwens uit dezelfde stal: www.storagecraft.com. We starten onze workshop met ShadowSurfer, waarvan je een volledig werkende versie vindt op de Clickx-cd bij dit nummer. Enkel in de laatste stap neemt ShadowUser Pro het roer over, ten behoeve van de meer veeleisende gebruiker. Een demoversie hiervan staat eveneens op onze cd.

## STAP 1 / INSTALLEREN

De installatie van ShadowSurfer heeft weinig om het lijf (zie afbeelding 1). Je hoeft slechts een vijftal keren op **Next** te drukken, waarna je de procedure afrondt met **Install** en **Finish**. Wel moet je na de eerste **Next** de licentieovereenkomst accepteren, beslis je na de derde **Next** of je de tool enkel voor jezelf dan wel voor elke gebruiker installeert, en kan je na de vierde **Next** nog de installatiemap aanpassen. Vooraleer je echt met het product aan de slag kan, moet je ook nog even Windows herstarten. Na de herstart verschijnt er een kader op je scherm. Druk op de knop **Activate** en typ de volgende Clickx-code in: 0C1D-7724-E8AD-F783-0371 (0 is het cijfer nul, niet de letter 'o'!). Klik op **OK** en ShadowSurfer is klaar voor gebruik!




*Haal ShadowSurfer gewoon van de Clickx-cd.*

## STAP 2 / SHADOWSURFER OPENEN

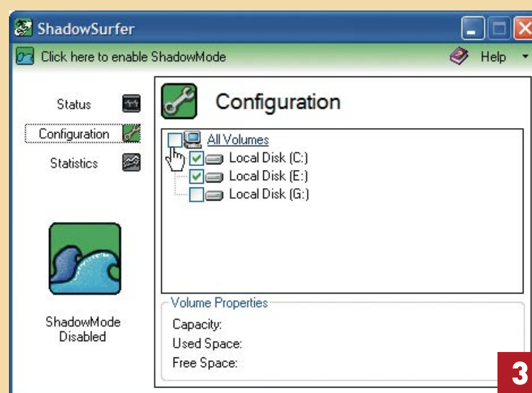
Zodra je Windows herstart hebt, verschijnt er een extra icoontje, uiterst rechts in de Windows-taakbalk. Hou je even de muispijl boven dit pictogram, dan lees je – naast een foutief versienummer; het gaat namelijk om versie 2.5 en niet om versie 2.0 – meteen de status van ShadowSurfer af (zie afbeelding 2). Op dit moment staat die nog ingesteld op **ShadowMode disabled**, wat zoveel betekent als: Windows werkt doodnormaal, en alle wijzigingen in het systeem zetten zich effectief door. De bedoeling is echter dat je een proefbed opmaakt om veilig te kunnen rollebollen. Dubbelklik daarvoor op het pictogram, zodat het programmavenster van ShadowSurfer te voorschijn komt. Dit venster kan je trouwens ook oproepen via de Windows **Start**-knop, waarna je achtereenvolgens **Alle programma's**, **ShadowSurfer**, **ShadowSurfer** aanklikt. Vooraleer we de **ShadowMode** in het venster activeren, lopen we echter eerst even langs de **Configuration**-knop...

*Nog even wachten met je wilde experimenten...*




## STAP 3 / CONFIGUREREN

Deze knop hoeft je alvast niet af te schrikken: het enige wat je hier kan aanstippen, is welke schijfstations je met ShadowSurfer wil beveiligen (zie afbeelding 3). Je ziet in dit lijstje trouwens enkel hardeschijfpartities opduiken – geen usb-sticks bijvoorbeeld. We raden je alvast aan een vinkje te plaatsen naast het station waarop Windows geïnstalleerd is. Op deze partitie bevindt zich namelijk ook het register, en een beveiliging met ShadowSurfer heeft weinig zin als dit onderdeel niet 'schrijfbeveiligd' is. Beschik je echter nog over een ander station, dan kan het handig zijn om dat juist niét te beveiligen. Tijdens een geactiveerde ShadowMode kan je dan naar dat station nog altijd bestanden wegschrijven die je absoluut wenst te behouden.

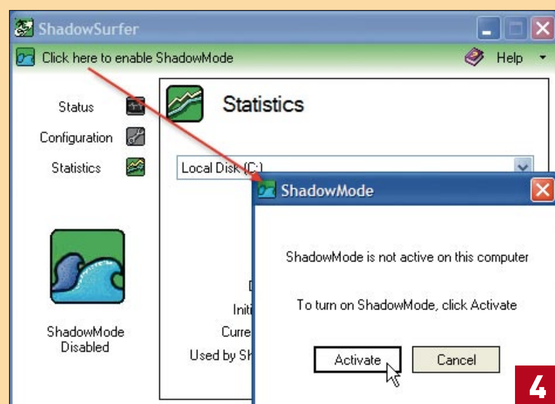



*Welke stations wil je 'schrijfbeveiligen'?*

## STAP 4 / SHADOWMODE ACTIVEREN

Het grote moment is aangebroken. Zodra je bovenaan op **Click here to enable ShadowMode** klikt en die keuze bevestigt met de knop **Activate** (zie afbeelding 4), hoef je enkel nog Windows te herstarten om over te schakelen naar die beveiligde modus. Een venstertje laat je de keuze of je meteen wil herstarten (**Reboot Now**) dan wel op een later moment (**Reboot Later**). Hoe dan ook, meteen na de herstart laat het behangpapier van je bureaublad er geen twijfel over bestaan dat de ShadowMode geactiveerd is. Dat zie je trouwens ook aan het ingekleurde icoontje op de Windows-taakbalk. Letterlijk alles wat je nu doet – en waarbij beveiligde stations betrokken zijn – wordt door ShadowSurfer

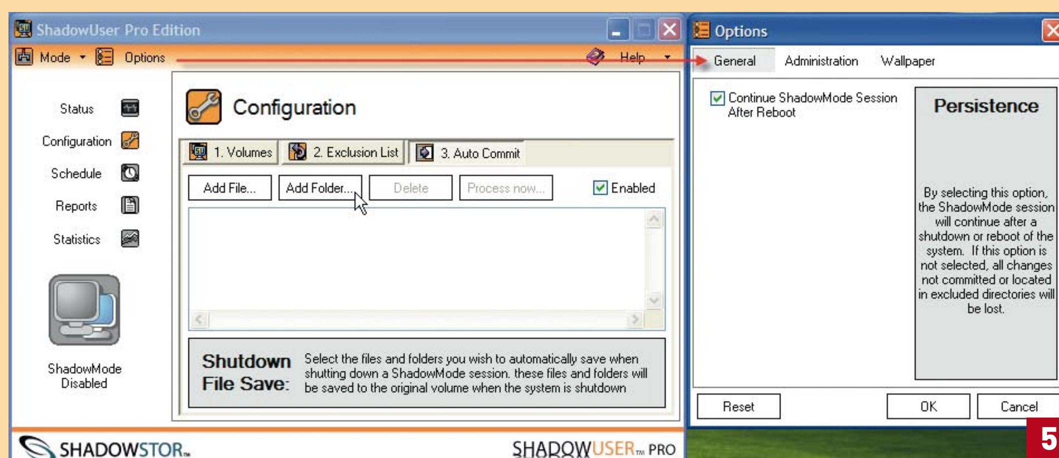
veilig afgevangen. En zodra je Windows herstart (!), schiet van al die wijzigingen geen bit meer over: weg virussen, weg nieuwe installaties, weg gewijzigde registersleutels, welkom verwijderde bestanden…




*Breng het testcircuit in gereedheid…*

## STAP 5 / SHADOWUSER PRO

Een herstart ruimt bij ShadowSurfer dus onverbiddelijk alle sporen van je experimenten in ShadowMode op. Dat is misschien minder handig als je bepaalde wijzigingen toch graag had behouden. Dat kan perfect met ShadowUser Pro (na 30 dagen proefversie betaal je hiervoor circa € 55). De installatie en de werking lopen volledig parallel aan die van kleine broer ShadowSurfer; alleen biedt het hoofdvenster heel wat bijkomende opties (zie afbeelding 5). Het is bijvoorbeeld mogelijk de (de)activering van de ShadowMode in te plannen, je kan er voor zorgen dat bepaalde bestand(smapp)en bij het afsluiten van het systeem toch effectief worden weggeschreven, en de ShadowMode kan ook na een herstart van Windows actief blijven – tot wanneer je die modus eigenhandig deactiveert. Op www.storagecraft.com/documents/SUguide.pdf vind je een Engelstalige handleiding (39 blz.). Je moet wel eerst ShadowSurfer van je computer verwijderen vooraleer je ShadowUser kan installeren. ♦




*ShadowUser Pro is heel wat flexibeler!*

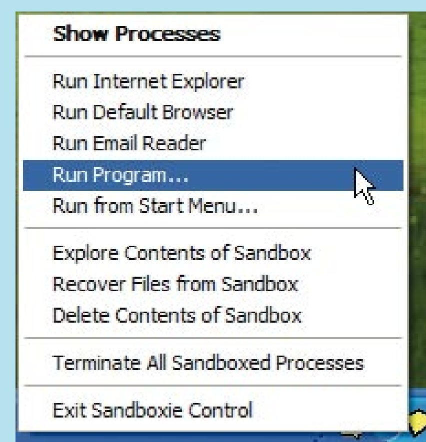
## ANDERE TESTCIRCUITS…

Er bestaan nog andere tools die min of meer op dezelfde leest geschoeid zijn als de twee producten van StorageCraft. Dat zijn onder meer DeepFreeze www.faronics.com, Skanix Illusion www.skanix.nl en Clean Slate www.fortres.com. Elk van deze tools kan je tevens in een netwerkversie aanschaffen, waarbij je de tool vanuit een centrale module op het netwerk kan beheren. In een eerdere test kwam Clean Slate wegens een treffelijke prijs (circa € 46) én een overtuigende flexibiliteit als winnaar van dit trio uit de bus. Sinds kort kan je voor een vergelijkbare – zij het iets minder flexibele – tool ook gratis bij Microsoft terecht: Windows Disk Protection, een onderdeel van de Shared Computer Toolkit www.microsoft.com/netherlands/windowsxp/sharedaccess.

Sandboxie (www.sandboxie.com – gratis te gebruiken, maar na 30 dagen word je herinnerd aan de registratie – circa € 16) kan je tot op zekere hoogte eveneens tot dit slag software rekenen. Deze tool werkt echter enkel op bestandsniveau en is dus minder omvattend dan de hierboven vermelde producten. Wij stelden ook een merkbare vertraging vast, en de software trakteerde ons testtoestel tevens op een paar vastlopers.

Er bestaat verder ook speciale hardware in de vorm van een insteekkaart, die dergelijke functies heeft ingebakken. Maar in de praktijk blijken die kaarten wel eens vaker incompatibiliteiten te vertonen. Bekende exemplaren zijn alvast de Reborn Card www.reborn.nl, Juzt-Reboot www.juzt-reboot.com en Boot & Go www.bootandgo.com.

Je kan het natuurlijk ook over een andere boeg gooien, en zogenoemde virtualisatiesoftware installeren. Dat zijn tools die een complete virtuele pc simuleren binnen je eigen systeem, net alsof je een aparte computer zou opstarten. Elke wijziging blijft dus geheel binnen de contouren van deze 'virtuele' pc, en bovendien kan je op elk moment een zogenaamd 'snapshot' maken. Zodra je dan naar zo'n snapshot terugkeert, worden wijzigingen die je nadien had uitgevoerd, automatisch weer ongedaan gemaakt. De bekendste tools zijn VMware www.vmware.com en Microsoft Virtual PC www.microsoft.com/windows/virtualpc. Van beide kan je gratis een proefversie downloaden.




*Sandboxie stopt alles in een zandbak*